СЕКЦИЯ 3.
ОРГАНИЗАЦИОННОЕ И ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

УДК 336. 719+006.44

Н. Д. Андрущук
Научный руководитель: д-р тех. наук, проф. В. Л. Кузнецов
Московский государственный технический университет
гражданской авиации, Москва

РАЗРАБОТКА АРХИТЕКТУРЫ ДЕЯТЕЛЬНОСТИ ПО ОБЕСПЕЧЕНИЮ НЕПРЕРЫВНОСТИ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ФУНКЦИОНИРОВАНИЯ БАНКА

Аннотация. Объектом исследования является деятельность по обеспечению непрерывности и информационной безопасности функционирования банка. В работе предпринята попытка разработки единой архитектуры данного вида деятельности в соответствии с требованиями комплекса стандартов Банка России и лучших практик вне зависимости от выбранной конкретной организацией банковской системы группы банковских операций. Подходы, примененные в работе, основаны на терминологическом и информационном методах анализа документов.

Ключевые слова: обеспечение информационной безопасности организации; методическая документация; методические рекомендации; управление рисками; управление инцидентами.

Необходимость совершенствования безопасности банковской системы обусловлена успешным развитием как банковской системы в целом, так и по-

вышением эффективности деятельности и устойчивости функционирования отдельных банков.

Такие факторы, как улучшение качества корпоративного управления, включая достижение большей прозрачности деятельности банков, эффективности риск-менеджмента, совершенствование отношений органов управления банков, акционеров и заинтересованных лиц, в значительной степени могут способствовать достижению цели повышения эффективности совершенствования безопасности банковской системы.

Формирование и дальнейшее улучшение банками систем управления рисками, приближение их к соответствующим международным стандартам позволяет уменьшить подверженность банковского сектора рискам, принимаемым на себя.

Разработка архитектуры. Исходя из существующих определений процесса в целом и бизнес-процесса в частности, мы можем рассматривать деятельность по обеспечению непрерывности и информационной безопасности (ОНиИБ) функционирования банка именно как процесс, предъявляя к нему соответствующие требования.

При этом под **процессом** будем понимать совокупность взаимосвязанных или взаимодействующих видов деятельности, преобразующую входы в выходы и требующую для этого определенных ресурсов и управляющих воздействий (управления). Входами к процессу обычно являются выходы других процессов. Однако входами могут быть и специфические требования, предъявляемые как к процессу в целом, так и к отдельным видам деятельности, ресурсов или управления. Такое определения понятия «процесс» позволяет осуществить определенную классификацию, подразделяющую рассматриваемый процесс ОНиИБ на следующие основные категории.

Основные процессы — процессы, обеспечивающие намеченный результат деятельности организации.

Вспомогательные процессы — процессы, предназначенные для обеспечения нормального функционирования основных и других процессов необходимыми ресурсами. В большинстве случаев обеспечение информационной безопасности (ОИБ) относится к вспомогательной деятельности. Однако очевидно, что при рассмотрении предложенной темы, необходимо изучать ОИБ именно как основной процесс, в дальнейшем выделяя в нем вспомогательные.

Процессы управления (менеджмента), относящиеся к стратегическому планированию, постановке целей и установлению политик, обеспечению коммуникаций и т. п.

Процессы измерения, анализа и совершенствования. Назначением данной группы процессов является предоставление входных данных для процессов усовершенствования деятельности организации в целом. Результатом

осуществления данных процессов будет выступать совершенствование всей деятельности организации [1, 2].

Данные определения позволяют принять за основу уже существующую архитектуру деятельности по обеспечению ИБ организации в соответствии со стандартом СТО БР ИББС-1.0–2014 «Обеспечение информационной безопасности организации банковской системы Российской Федерации. Общие положения» [3].

Для реализации, эксплуатации, контроля и поддержания на должном уровне системы обеспечения информационной безопасности (СОИБ) в организации банковской системы России (БС РФ) следует реализовать ряд процессов системы менеджмента информационной безопасности (СМИБ), сгруппированных в виде циклической модели Деминга: «… — планирование — реализация — проверка — совершенствование — планирование — …».

Целью выполнения деятельности в рамках группы процессов «планирование» является запуск «цикла» СМИБ путем определения первоначальных планов построения, ввода в действие и контроля СОИБ, а также определения планов по совершенствованию СОИБ на основании решений, принятых на этапе «совершенствование».

Этап «реализация» осуществляется по результатам реализации этапов «планирование» и (или) «совершенствование» и заключается в выполнении всех планов, связанных с построением, вводом в действие и совершенствованием СОИБ, определенных на этапе «планирование» и (или) реализации решений, определенных на этапе «совершенствование» и не требующих выполнения деятельности по планированию соответствующих улучшений.

Целью выполнения деятельности в рамках группы процессов «проверка» является обеспечение достаточной уверенности в том, что СОИБ, включая защитные меры, функционирует надлежащим образом и адекватна существующим угрозам информационной безопасности (ИБ), а также внутренним и (или) внешним условиям функционирования организации БС РФ, связанным с ИБ [4].

Аналитические результаты, полученные при изучении деятельности по ОНиИБ функционирования банка, проведенные первичная систематизация и структуризация существующих направлений деятельности говорят о необходимости расширения и усовершенствования действующей архитектуры с учетом предлагаемых изменений в соответствии с требованиями комплекса стандартов Банка России и лучших практик.

Структурирование понятия деятельности по ОНиИБ функционирования банка позволяет представить в общем виде сложность задач построения системы банковской защиты. Функционирование многоуровневой системы защи-

ты обеспечивается применением мер правового, организационного, сыскного, криминалистического характера.

Создание такой системы защиты на практике связано с решением широкого и разнопланового набора проблем. В их числе задачи разработки стратегии и тактики обеспечения безопасности банка; структурирование и уточнение целей и задач обеспечения безопасности; разработка комплекса основных мер, направленных на достижение указанных целей; подготовка предложений по совершенствованию правового, нормативно-методического, научно-технического и организационного обеспечения безопасности [5].

Список литературы

1. ГОСТ Р ИСО/МЭК ТО 18044–2007 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности». М. : Стандартинформ, 2009.

2. ГОСТ Р ИСО/МЭК 27005–2010 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности», М. : Стандартинформ, 2011.

3. Стандарт Банка России СТО БР ИББС-1.0–2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения».

4. Рекомендации в области стандартизации Банка России РС БР ИББС-2.2–2009 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки рисков нарушения информационной безопасности».

5. ISO/IEC27035:2011 «Information Technology. Security Techniques. Information Security Incident Management».

УДК 004.056.53

А. А. Бабкина
Научный руководитель: канд. пед. наук, доц. О. Р. Уторов
Южно-Уральский государственный университет, Челябинск

УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ «ОПЛАТЕ В ОДНО КАСАНИЕ»

Аннотация. В статье рассматриваются актуальные угрозы информационной безопасности при предоставлении банками функций безналичного расчета так называемого «в одно касание» без ввода ПИН-кода с помощью мобильного телефона в приложениях «AndroidPay», «ApplePay», «SamsungPay» и др. Раскрывается один